Notice of Allowability	Application No.	Applicant(s)	
	09/543,056	SIMON	
	Examiner	Art Unit	
	Justin T. Darrow	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *an amendment after final rejection filed 10/12/2004*.

2. ☒ The allowed claim(s) is/are *7,8,15,16,25 and 35*.

3. ☒ The drawings filed on *05 April 2000* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

1. Claims 1-37 have been presented for examination. Claims 1-6, 9-14, 17-24, 25-34, 36, and 37 have been canceled and claim 35 has been amended in an amendment after final rejection filed 10/12/2004). Claims 7, 8, 15, 16, 25, and 35 have been examined.

Docketing

2. This application has been docketed to Primary Examiner Justin T. Darrow in Group Art Unit 2132 in Technology Center 2100.

Response to Amendment

3. The amendment after final rejection filed 10/12/2004 will be entered in its entirety.

Allowable Subject Matter

4. Claims 7, 8, 15, 16, 25, and 35 are allowed.

5. The following is an examiner's statement of reasons for allowance:

Claims 7 and 8 are drawn to a system supporting public key encryption. The closest prior art, Goldschlag et al., U.S. Patent No. 6,108,644 A, discloses a similar method. Goldschlag et al. describe a system supporting public key encryption comprising:

a certifying authority (see column 5, lines 57-60; a registrar to validate an unvalidated certificate);

a client device, coupled to the certifying authority (see column 6, lines 3-7; a customer in communication with the registrar), to

generate a blinded certificate (see column 2, lines 22-25; the customer applies a blinding factor to a nonce to submit to a certification authority; see column 5, lines 45-55; figure 1, step 101; where the blinded unvalidated certificate is the hashed nonce combined with the blinding factor that the customer submits to the registrar), and

transmit the blinded certificate to the certifying authority (see column 5, lines 45-55; figure 1, step 101; the registrar receives the blinded unvalidated certificate from the customer);

where the certifying authority is to digitally sign the blinded certificate according to a formula

(blinded certificate)^d mod (n), (see column 5, lines 57-60; figure 1, step 103; validating the blinded unvalidated certificate by signing it; see column 2, lines 62-67; column 3, lines 1-4; where the certificate is signed with a private key corresponding to publicly available verification key)

wherein the certifying authority is to encode a security attribute into the digital signature (see column 5, lines 60-67; figure 1, step 104; the registrar party atomically binds the blinded validated certificate to a secret encrypted session key as a security attribute).

However, Goldschlag et al. neither teach nor suggest:

identifying, for each bit in a series representing the security attribute that has a particular value, a corresponding integer; and

generating as the value *d* the product of the identified integers.

This combination of features explicitly incorporated into independent claim 7 render claims 7 and 8 allowable.

Claims 15 and 16 are drawn to a method. The closest prior art, Goldschlag et al., U.S. Patent No. 6,108,644 A, discloses a similar method. Goldschlag et al. describe a method comprising:

receiving, from a client, a current certificate and a request to sign a new certificate (see column 6, lines 58-64; figure 2, step 202; the first party, registered customer, sends a transaction request message to the second party, vendor, atomically binding an unblended certificate as a current certificate, and a blinded unvalidated certificate to be validated as a new certificate to by signed);

determining attributes of the client based on the current certificate (see column 7, lines 12-15; the vendor performs a one-way hash function of the nonce N_i included in the request as an attribute of the client, and compares the result to the validated unblended hashed nonce h (N_i) as the current certificate); and

digitally signing the new certificate using a private key (see column 7, lines 18-23; the vendors validates the blinded hashed nonce of the request message as the new certificate to be signed);

where digitally signing comprises calculating the value of a formula

(blinded certificate)^d mod (n), (see column 2, lines 62-67; column 3, lines 1-4; where the certificate is signed with a private key corresponding to publicly available verification key).

However, they neither show nor imply:

selecting, in accordance with public key cryptography, a public/private key pair that is based at least in part on the attributes of the client;

where selecting comprises:

representing the attributes as a series of bits;

identifying, for each bit in the series that has a particular value, corresponding integer; and

generating as the value *d* the product of the identified integers.

This sequence of steps explicitly recited in independent claim 15 renders claims 15 and 16 allowable.

Claims 25 and 35 are drawn to a method and one or more computer-readable media containing a plurality of instructions, respectively. The closest prior art, Goldschlag et al., U.S. Patent No. 6,108,644 A, discloses a similar method and media. Goldschlag et al. describe a method and media for comprising:

receiving, from a client, a request for electronic content (see column 6, lines 58-60; figure 2, step 202; a transaction request message is received from a registered customer; see column 1, lines 46-48 and 66-67; column 2, lines 1-4; where the transaction concerns a request for a product including providing any kind of electronic information);

checking, based on information encoded in a digital signature of at least a portion of the request, whether the client has a set of claimed security attributes (see column 7, lines 12-15; the vendor performs a one-way hash function of the nonce N_i included in the transaction request as

an attribute of the client, and compares the result to the validated unblinded hashed nonce h (N_i) as the digital signature; see column 5, lines 57-60; figure 1, step 103; validating the blinded unvalidated certificate by signing it to form a digital signature; see column 6, lines 53-55; figure 2, step 201; which the registered customer unblinds);

using a public key to verify the digital signature (see column 6, lines 65-66; figure 2, step 203; determining if the unblended certificate is valid; see column 2, line 67; column 3, line 1-4; by using a publicly available verification key in a transaction where the customer requests a product) and

determining how to respond to the request based on the checking (see column 7, lines 15-18; if the result and the validated unblinded hashed nonce h (N_i) as the digital signature correspond, the vendor determines that the validated unblended hashed nonce is a valid certificate, sends an approval message, and engages in the transaction).

However, they neither teach nor motivate:

representing the set of claimed security attributes as a series of bits; and

generating a public key for a certifying authority using the series of bits;

where generating comprises:

identifying, for each bit in the series that has a particular value, corresponding integer; and

generating as the public key the product of the identified integers.

This combination of steps explicitly recited in independent claims 25 and 35 renders them, respectively, allowable.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- S. Stubblebine, P. Syverson, and D. Goldschlag, "Unlinkable Serial Transactions: Protocols and Applications," disclose a subscription chain formed from a sequence of certificates used for performing similar tranactions

Telephone Inquiry Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Justin T. Darrow whose telephone number is (571) 272-3801, and whose electronic mail address is justin.darrow@uspto.gov. The examiner can normally be reached Monday-Friday from 8:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón, Jr., can be reached at (571) 272-3799.

The fax number for Formal or Official faxes to Technology Center 2100 is (703) 872-9306. In order for a formal paper transmitted by fax to be entered into the application file, the paper and/or fax cover sheet must be signed by a representative for the applicant. Faxed formal

papers for application file entry, such as amendments adding claims, extensions of time, and statutory disclaimers for which fees must be charged before entry, must be transmitted with an authorization to charge a deposit account to cover such fees. It is also recommended that the cover sheet for the fax of a formal paper have printed "**OFFICIAL FAX**". Formal papers transmitted by fax usually require three business days for entry into the application file and consideration by the examiner. Formal or Official faxes including amendments after final rejection (37 CFR 1.116) should be submitted to (703) 872-9306 for expedited entry into the application file. It is further recommended that the cover sheet for the fax containing an amendment after final rejection have printed not only "**OFFICIAL FAX**" but also "**AMENDMENT AFTER FINAL**".

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (571) 272-2100 thereafter.

November 13, 2004

JUSTIN T. DARROW
PRIMARY EXAMINER
TECHNOLOGY CENTER 2100